Washington Journal of Law, Technology & Arts

Volume 16 | Issue 2 Article 2

3-19-2021

Digital Contract Tracing in the Workplace

Alexandra Kiosse
Fordham University School of Law

Digital Contract Tracing in the Workplace

Cover Page Footnote

J.D. Candidate, 2022, Fordham University School of Law; B.A., 2019, Binghamton University.

I would like to thank Professor Olivier Sylvain and the editors and staff of the Washington Journal of Law, Technology & Arts. I would also like to thank my family and friends, in particular Lucjan for his unending encouragement and support.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 16, ISSUE 2 WINTER 2021

DIGITAL CONTRACT TRACING IN THE WORKPLACE

Alexandra Kiosse [*]

CITE AS: A KIOSSE, 16 WASH. J.L. TECH. & ARTS 1 (2021) *https://digitalcommons.law.uw.edu/wjlta/vol16/iss2/2*

ABSTRACT

The COVID-19 pandemic has affected the way businesses run and operate in the United States. With the dire need to keep employees safe, digital contact tracing has become the most efficient mechanism for controlling the spread of the virus within places of employment. However, information privacy laws come into tension with the use of employee health data by employers and third parties. This Article proposes a careful balance between contact tracing and maintaining employees' privacy as they share health and proximity data with digital contact tracing applications in the workplace.

TABLE OF CONTENTS

[**] J.D. Candidate, 2022, Fordham University School of Law; B.A., 2019, Binghamton University. I would like to thank Professor Olivier Sylvain and the editors and staff of the Washington Journal of Law, Technology & Arts. I would also like to thank my family and friends, in particular Lucjan for his unending encouragement and support.

1. INTRODUCTION

When the deadly smallpox virus was eliminated worldwide after centuries of infection, popular belief dictated that its eradication was due to global immunization.[1] In reality, it was extensive

[1] *History of Smallpox*, CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/smallpox/history/history.html (last visited Nov. 1, 2020); *Contact Tracing*, CLIMATE CHANGE AND PUB. HEALTH L. SITE AT LA. STATE UNIV. https://biotech.law.lsu.edu/Books/lbb/x578.htm (last visited Nov. 1, 2020) [hereinafter *Contact Tracing*].

contact tracing that facilitated the eradication of smallpox.[2] At the time, contact tracing depended on a team of investigators interviewing the patient, along with the patient's family, friends, and any other people who may have known of the patient's close contacts who may have been exposed.[3] The patient's close contacts were discerned and were then subjected to control measures such as quarantine, vaccination, or treatment.[4] Now, forty years after the success of smallpox contact tracing, digital contact tracing has taken over as a cost-effective and less labor-intensive technological upgrade.[5] In light of the COVID-19 pandemic, digital contact tracing can be used to stop or slow down the spread of the virus.[6]

However, the emergence of digital contact tracing applications and mechanisms in the workplace can have far reaching implications for the health privacy of employees. Unresolved questions are raised, especially regarding whether employers will be able to access their employees' location data, various symptoms and health information, and the data of employees' close contacts.[7] Digital contact tracing may also implicate various information privacy principles and laws, as well as privacy provisions found within statutes like the Americans with Disabilities Act ("ADA"). Although there are privacy issues associated with digital contact tracing that the United States may not be prepared to address, employers will likely opt to use these mechanisms.[8]

---

[2] *Contact Tracing*, *supra* note 1.
[3] *Digital Contact Tracing*, CORONAVIRUS TODAY https://www.coronavirustoday.com/digital-contact-tracing (last visited Nov. 26, 2020) [hereinafter *Digital Contact Tracing*].
[4] *Id.*
[5] *Tracking COVID-19: Contact Tracing in the Digital Age*, WORLD HEALTH ORG. (Sept. 9, 2020), https://www.who.int/news-room/feature-stories/detail/tracking-covid-19-contact-tracing-in-the-digital-age.
[6] *Id.*
[7] *Digital Contact Tracing*, *supra* note 3.
[8] Andy Green, *Complete Guide to Privacy Laws in the U.S.*, VARONIS (March 29, 2020), https://www.varonis.com/blog/us-privacy-laws/ (noting that there is no federal privacy law that can force companies to issue and comply with privacy policies).

Due to stay-at-home orders in 2020, more than half of small businesses in the United States had temporarily closed.[9] As businesses began to reopen their doors, employers had the difficult task of preventing a COVID-19 outbreak, which would likely shut certain businesses down for good.[10] With several big businesses opting for digital contact tracing to keep their workplace COVID-19-free, as well as the release of a digital contact tracing application by Apple and Google, questions of privacy and personal health information are especially urgent.[11]

Part I of this Article discusses the framework of information privacy principles that make up the privacy laws in the United States, examines notable regulations and statutes regarding the privacy of health information, and analyzes their connection to each other. Part II demonstrates the potential negative impact of digital contact tracing tools in the workplace; namely, the potential threats to employee privacy. Finally, Part III attempts to mitigate privacy concerns, and proposes making COVID-19 a disability under the ADA, passing a federal law with common information privacy principles incorporated, and facilitating communication between employers and federal and local health agencies.

I. CURRENT PROTECTIONS FOR HEALTH INFORMATION PRIVACY

[9] Andrew Soergel, *More Than Half of Small Businesses Closed Temporarily Amid Coronavirus Outbreak*, U.S. NEWS (May 5, 2020), https://www.usnews.com/news/economy/articles/2020-05-05/more-than-half-of-small-businesses-closed-temporarily-amid-coronavirus-outbreak.

[10] *See generally*, Anne Sraders & Lance Lambert, *Nearly 100,000 Establishments that Temporarily Shut Down Due to the Pandemic are Now Out of Business*, FORTUNE (Sept. 28, 2020), https://fortune.com/2020/09/28/covid-buisnesses-shut-down-closed/.

[11] *Apple and Google Partner on COVID-19 Contact Tracing Technology*, APPLE NEWSROOM (Apr. 10, 2020), https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/; *see also*, Kif Leswing, *As Workplaces Slowly Reopen, Tech Companies Smell a New Multi-Billion Dollar Opportunity: Helping Businesses Trace Coronavirus*, CNBC (May 10, 2020), https://www.cnbc.com/2020/05/10/coronavirus-tracing-for-workplaces-could-become-new-tech-opportunity.html.

The Personal Identifiable Information ("PII") of employees is protected by several different mechanisms. These include information privacy principles that federal laws, federal regulations, and state laws are based on.[12] These principles, laws, and regulations work concurrently with federal statutes and regulations geared toward medical and health information specifically, such as the ADA and advisory opinions and regulations promulgated by the Centers for Disease Control ("CDC") and the Equal Employment Opportunity Commission ("EEOC"). Part I.A discusses the Fair Information Practice Principles, notable information privacy statutes, and federal bills as they relate to digital contact tracing for the COVID-19 pandemic. Part I.B discusses the EEOC and the ADA's protections for employees' medical information. Part I.C examines how employers may use digital contact tracing applications to track COVID-19 in the workplace and protect employees from infection.

A. The Fair Information Practice Principles and U.S. Information Privacy Law

While the U.S. Constitution protects certain aspects of privacy, and there are "sector- and harm-specific privacy laws," there is no general comprehensive federal law governing information privacy in the United States.[13] However, the Fair Information Practice Principles ("FIPPs") act as guiding privacy values that are widely incorporated into United States privacy law.

1. History of the Fair Information Practice Principles

The FIPPs are a set of widely accepted and internationally recognized principles that serve as the basis for information privacy policies within the government and the private sector in the

---

[12] *See generally Fair Information Practice Principles*, FED. TRADE COMM'N (Mar. 31, 2009), https://web.archive.org/web/20090331134113/http:/www.ftc.gov/reports/privacy3/fairinfo.shtm.

[13] Lothar Determann, *Healthy Data Protection*, 26 MICH. TELECOMMS. AND TECH. L. REV. 229, 241 (2020).

United States and abroad.[14] The FIPPs' core principles were modeled after the Organization for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[15] The OECD is an international organization geared toward shaping policy for a range of social and economic issues, including work on privacy policy and the FIPPs, which were written in 1980.[16] Congress first incorporated the FIPPs into the Fair Credit Reporting Act, which promotes "accuracy, fairness, and privacy" of information in files of consumer reporting agencies, including credit bureaus and agencies that sell information about medical records, rental history records, and check writing histories.[17] The FIPPs were also

---

[14] NAT'L PUBLIC SAFETY P'SHIP, THE FAIR INFO. PRACTICE PRINCIPLES (FIPPS) IN THE INFORMATION SHARING ENVIRONMENT (ISE) 1, https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf =; DEP'T OF HOMELAND SEC., 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM (2008). The Department of Homeland Security is one of the federal departments and agencies that have adopted the FIPPs. *Id.*

[15] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORG. ECON. CO-OPERATION & DEV. [hereinafter OECD Guidelines] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited Oct. 3, 2020) [hereinafter OECD Guidelines]; Frederik Zuiderveen Borgesius, Jonathan Gray & Mireille van Eechoud, *Open Data, Privacy, and Fair Information Principles: Towards A Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2102 (2015); *see Members and Partners*, ORG. ECON. CO-OPERATION & DEV., http://www.oecd.org/about/membersandpartners (last visited Oct. 3, 2020) for a list of OECD member countries. The OECD, an intergovernmental economic organization with thirty-seven member countries, expanded on the original four FIPPs and adopted a more comprehensive version of eight principles in 1980. *Id*.; Erin Corken, *The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future*, 42 N. KY. L. REV. 287, 291 (2015).

[16] *OECD Privacy Guidelines*, ORG. ECON. CO-OPERATION & DEV., http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm (last visited Nov 22, 2020).

[17] Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x (2012)); see FED. TRADE COMM'N, A SUMMARY OF YOUR RIGHTS UNDER THE FAIR CREDIT REPORTING ACT, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-

incorporated into the Privacy Act of 1974, which established fair information practices governing "the collection, maintenance, use, and dissemination of information" maintained in federal agency records.[18] Years later, the Federal Trade Commission ("FTC") and the Obama Administration called for FIPPs-centered privacy regulation in the public and private sectors.[19] Through studies of methods implemented by entities to collect, use, and safeguard personal information, the FIPPs continued to evolve.[20] Now the FIPPs are widely utilized by various federal agencies and are used as the framework for state privacy laws. The five commonly accepted FIPPs in the United States, as formulated by the FTC, include: (1) notice/awareness; (2) choice/ consent; (3) access/ participation; (4) integrity/ security; and (5) enforcement/ redress.[21]

---

act.pdf (last visited 11/5/2020) for more information about the Fair Credit Reporting Act.

[18] 5 U.S.C. § 552a; DEP'T OF JUSTICE, PRIVACY ACT OF 1974, https://www.justice.gov/opcl/privacy-act-1974 (last updated Jan. 15, 2020); DEP'T OF HOMELAND SEC., 2008-02, PRIVACY POLICY GUIDANCE MEMORANDUM (2008).

[19] *See generally* Borgesius et al., *supra* note 15, at 2101–08, for the background and history of the FIPPs in the United States and abroad; OFF. OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012); OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB MEMORANDUM M-13-13, OPEN DATA POLICY – MANAGING INFORMATION AS AN ASSET (May 9, 2013) (delineating implementation guidance material for former President Obama's 2013 executive order).

[20] Nicholas Camillo & Devika Kornbacher, *Fair Information Practice Principles in Data Privacy Law*, 2019 ADVANCED INTELL. PROP. L. 3.2, 2019 WL 8275404.

[21] *Fair Information Practice Principles*, FED. TRADE COMM'N (Mar. 31, 2009), https://web.archive.org/web/20090331134113/http:/www.ftc.gov/reports/privacy3/fairinfo.shtm. The five FIPPs that will be discussed in this Artcileote are formulated by the FTC as the principles common to all regulations and guidance related to the FIPPs. *Id.*; *cf.* Corken, *supra* note 15, at 291 (citing OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Org. Econ. Co-Operation & Dev., http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyan); cf. DEP'T OF HOMELAND SEC., *The Fair Information Practice Principles at Work* (June 2011),

Data minimization is also a common principle used to rein in entities' data collection policies.[22]

2. The Fair Information Practice Principles Explained

The notice and awareness principle dictates that individuals should receive notice of an entity's information practices prior to the collection of their personal information.[23] This ensures that individuals can make informed decisions as to whether to disclose the information sought, and to what extent to disclose it.[24] The FTC recommends the issuance of understandable and concise privacy notices divulging the identification of the entity collecting the data, the uses of the data, the recipients of the data, the nature and means of the data collection, and the steps taken to ensure confidentiality, integrity, and quality of the data.[25] Entities may also be required to identify any choice individuals have regarding the use of their data, their rights to access the data and correct any inaccuracies, and the availability of redress for violations of the respective information privacy policy.[26] Meaningful notice and

---

https://www.dhs.gov/sites/default/files/publications/dhsprivacy_fippsfactsheet.pdf (discussing the FIPPs as formulated and utilized in DHS privacy practices).

[22] *Data Minimization*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/Data-Minimization (last visited Nov. 22, 2020).

[23] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter A Report to Congress].

[24] *Id.*; Corken, *supra* note 15, at 290.

[25] *See*, e.g., A Report to Congress, *supra* note 23; Ben Davis, *GDPR: How to create best practice privacy notices (with examples)* (July 17, 2017), https://econsultancy.com/gdpr-best-practice-privacy-notices-examples/. The GDPR is the European Union's privacy and security law utilizing data protection principles similar to the FIPPs, including transparency to individuals. Ben Wolford, *What is GDPR, the EU's new data protection law?*, https://gdpr.eu/what-is-gdpr/?cn-reloaded=1 (last visited Dec. 5, 2020).

[26] A Report to Congress, *supra* note 23; David Hoffman & Paula J. Bruening, *Rethinking Privacy: Fair Information Practice Principles Reinterpreted* 13–14, INTEL, https://bigdata.fpf.org/wp-content/uploads/2015/11/Intel-Rethinking-Privacy.pdf (last visited Dec. 5, 2020); *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 980 (2017) (noting that design, in addition to words, should also be considered when

awareness is required for the application of the remaining four FIPPs. Without it, individuals do not have knowledge regarding the use of their data, and thus are powerless to control it.[27]

The second FIPP, choice and consent, refers to individuals' ability to determine how any personal information collected from them can be used, especially regarding secondary uses of information.[28] Secondary uses of personal information are any uses beyond those "necessary to complete the contemplated transaction," including internal use within the entity or external use, when data is transferred to a third party.[29] Entities may apply opt-in or opt-out regimes to their privacy policies.[30] Opt-in regimes require individuals to affirmatively allow the collection and use of their information, and opt-out, or tacit consent, regimes require individuals to affirmatively forbid the collection and use of such information for internal or external uses.[31] Within these regimes, entities can offer individuals greater choice by allowing them to tailor the nature of the information collected and the uses that information will be put to by specifying their preferences.[32]

The access and participation principle refers to individuals' ability to access their own data, and to contest the accuracy or completeness of it.[33] The FTC recommends that access be timely, inexpensive, and relatively simple to give individuals a meaningful

---

deciding if the notice given was sufficient).

[27] *See, e.g.*, A Report to Congress, *supra* note 23; Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2049 n.29 (2000).

[28] A Report to Congress, *supra* note 23.

[29] *Id*.; *see also* Thomas Gallagher, Kudakwashe Dube & Scott McLachlan, *Ethical Issues in Secondary Use of Personal Health Information* (May 2018), https://cmte.ieee.org/futuredirections/tech-policy-ethics/may2018/ethical-issues-in-secondary-use-of-personal-health-information/ (discussing how personal health information may be used by third parties).

[30] A Report to Congress, *supra* note 23.

[31] *Id*.; Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies* (Dec. 16, 2005), https://www.econinfosec.org/archive/weis2006/docs/34.pdf.

[32] A Report to Congress, *supra* note 23.

[33] *Id*.; Pam Dixon, *A Brief Introduction to Fair Information Practices* (June 5, 2006), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (discussing the access/participation principle under the name "individual participation").

ability to see and change the data that was collected.[34]

The integrity and security principle recommends that data collectors take reasonable steps to ensure data integrity and protect against loss, unauthorized access, use, destruction, and disclosure of data.[35] This can be achieved by using reputable sources of data, complying with the access and participation principle to allow correction, destroying untimely data, and limiting third party access through the encryption and secure storage of collected information.[36]

Finally, enforcement and redress ensures that the FIPPs are implemented and individuals can obtain relief for violations.[37] These goals may be met by: (1) self-regulation, (2) government enforcement, and (3) private remedies.[38] Self-regulation in entities can include audits, which allow entities to link the misuse of information collected to a particular source.[39] This allows victims to get recourse and acts as a deterrent against the data abuser.[40] With an auditing mechanism, entities can investigate and compensate individuals for the harm suffered by the unauthorized collection or misuse of their information.[41] Government enforcement via federal agencies or legislation is also a means to redress data misuse and other data violations.[42] Such enforcement

---

[34] A Report to Congress, *supra* note 23.
[35] *Id*.; Dixon, *supra* note 33 (defining the integrity/security principle under the name "security safeguards principle").
[36] A Report to Congress, *supra* note 23; *see also* NATIONAL PUBLIC SAFETY PARTNERSHIP, *supra* note 14.
[37] A Report to Congress, *supra* note 23; Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J. L. & TECH. 149, 182 (2001).
[38] A Report to Congress, *supra* note 23.
[39] *Id*.
[40] *Id*.; FED. TRADE COMM'N, INDIVIDUAL REFERENCE SERVICES – A REPORT TO CONGRESS (1997).
[41] A Report to Congress, *supra* note 23.
[42] *Id*.; U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, SEC'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) https://www.hsdl.org/?view&did=479784 [hereinafter RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS] (advocating for the inception of a federal agency to regulate the use of all automated personal data systems); U.S. DEP'T OF HEALTH AND HUM. SERV., INFO. INFRASTRUCTURE TASK FORCE, INFO. POLICY COMM., PRIV. WORKING GROUP, PRIVACY AND THE

often comes from the FTC, which can levy penalties for unfair data practices.[43] Finally, private litigants can similarly rely on a statutory scheme that provides private rights to litigate.[44] Individuals harmed by the violation of information privacy practices or unfair data collection could thus recover via compensatory or punitive damages.[45]

Data minimization, as another regulatory principle related to privacy policy, involves limiting data collection to only what is required to fulfill a specific purpose.[46] Essentially, the principle requires that entities use only the least amount of data possible. With regard to contact tracing applications, this would require only the use of proximity data for the purpose of informing other users of the application that they had been in close contact with someone who tested positive or exhibited symptoms of COVID-19.[47]

3. Notable State Privacy Statutes and Bills

The five FIPPs are interrelated and work together in information privacy regulations, statutes, and policies binding federal agencies and private entities. Several states have adopted information privacy laws including the California Consumer Privacy Act ("CCPA").[48] Moreover, other states are entertaining bills that

---

NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995), https://aspe.hhs.gov/privacy-and-national-information-infrastructure-principles-providing-and-using-personal-information (noting regulatory enforcement and criminal prosecution as options for redress).

[43] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[44] A Report to Congress, *supra* note 23.; RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, *supra* note 42 (discussing the need for federal legislation and advocating for uniform state legislation).

[45] A Report to Congress, *supra* note 23.

[46] *Data Minimization*, *supra* note 22.

[47] Johannes Abeler et al., *COVID-19 Contact Tracing and Data Protection Can Go Together* (Apr. 20,2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7173240/.

[48] CAL. CIV. CODE § 1798.100 (West 2020).

resemble the CCPA.[49]

The CCPA applies to for-profit companies that do business in California, have a gross revenue of over twenty-five million dollars, buy, receive, or sell personal information of fifty thousand or more California residents, households, or devices, or derive 50 percent or more of their annual revenue from selling the personal information of California residents.[50] The CCPA operates via an opt-out regime, in which individuals have the right to delete personal information, request that entities not use personal information, and obtain notice regarding the type of personal information collected and how it is being used.[51] Any contract provision attempting to waive these rights is unenforceable.[52] Under the CCPA, personal information is broadly defined as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[53] As such, the CCPA includes employment related information.[54] As per new regulations that went into effect in August 2020, the CCPA requires entities to provide consumers with timely notice at the collection of data that should be understandable to consumers and inform them of the categories of data to be collected.[55] The notices must use plain, non-legal language, draw the consumers' attention to the notice, be available in multiple languages, and be accessible to viewers with disabilities.[56] Moreover, entities cannot collect data which the consumer was not given notice of, and consumers must be informed of their right to opt-out of collection.[57]

Following California's lead, New York and Massachusetts

---

[49] *See* S. 5642, 242d Leg. Sess. (N.Y. 2019); S. 120, 191st Sess. (Mass. 2019).
[50] CIV. § 1798.140(c).
[51] CIV. § 1798.100.
[52] CIV. § 1798.192.
[53] CIV. § 1798.140(o)(1).
[54] *Id.* at § 1798.140(o)(1)(I).
[55] California Consumer Privacy Act Regulations, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf? (last visited Dec. 20, 2020).
[56] *Id.*
[57] *Id.*

have proposed statutes that resemble the CCPA. New York's proposed privacy statute features the right to delete personal information, and request to see the personal information collected by an entity, like the CCPA.[58] Unlike the CCPA however, the proposed New York Privacy Act does not have a revenue threshold for businesses, creates a fiduciary relationship between businesses and the individuals whose data is used, and allows individuals to correct inaccurate information.[59] The proposed New York law was not passed in 2019, and is on "hold" as of October 2020.[60] The Massachusetts bill also shares language from the CCPA, and includes access to personal information, the right to delete information, the right to opt-out of the sale of information, and guaranteed notice of privacy rights.[61] Unlike the CCPA however, the Massachusetts bill provides a broader right of redress for individuals, regardless of monetary loss.[62]

4. Federal Privacy Bills

The COVID-19 pandemic has created a need for strong data privacy laws in collaboration with longstanding statutes that govern health information in the workforce, such as the ADA.[63] In response, there are two bills before Congress: the Public Health Emergency Privacy Act ("PHEPA"),[64] and the COVID-19 Consumer Data Protection Act ("CCDPA")[65].

The PHEPA governs any federal or private entity that

[58] S. 5642, 242d Leg. Sess. § 1103(3)(a) (N.Y. 2019)
[59] *Id*.
[60] Joanna Kessler, Note, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource"*, 93 S. CAL. L. REV. 99, 126 (2019) (citing Tim Sandle, *New York Lawmakers Reject Data Privacy Act in Surprise Turn*, DIGITAL J. (July 22, 2019), http://www.digitaljournal.com/tech-and-science/technology/new-york-lawmakers-reject-data-privacy-act-in-surprise-turn/article/554461 [https://perma.cc/32RR-6GF8]).
[61] S. 120, 191st Sess. (Mass. 2019).
[62] *Id*.
[63] 42 U.S.C. §§ 12111–12117.
[64] H.R. 6866, 116th Cong. (2020).
[65] S. 3663, 116th Cong. (2020).

"collects, uses, or discloses emergency health data" or that develops a website or an application for the purposes of contact tracing.[66] The proposed act incorporates several FIPPs. Data minimization is required to ensure that an entity only collects, uses, and discloses data that is "necessary, proportionate, and limited for a good faith public health purpose."[67] The access and participation principle in PHEPA ensures that the information collected by entities is accurate and that inaccurate information can be corrected by individuals.[68] Finally, reasonable safeguards are included in the bill to prevent unlawful discrimination on the basis of the health data collected.[69] The proposed act allows the disclosure of health data to the government when the disclosure is made to a public health authority in good faith.[70] Additionally, PHEPA prohibits the withholding of employment opportunities on the basis of emergency health data, requires express consent and clear and conspicuous notice, and creates private and regulatory forms of redress for violations of PHEPA.[71]

The CCDPA is much less broad. It prohibits entities from collecting, processing, or transferring covered data, including geolocation, proximity, identifiers, and personal health information, unless the entity provides prior notice and the individual expressly consents.[72] It also provides that entities must publish a clear and conspicuous privacy policy, practice data minimization, offer a right to delete and correct data, and establish a reasonable security mechanism.[73] Unlike the PHEPA, the CCDPA offers no private right of action, and preempts state law, so that states cannot pass any laws related to the "collection, processing, or transfer of covered data" involving tracking the spread of COVID-19, measuring compliance with social distancing guidelines, and conducting contact tracing.[74] The CCDPA also

[66] H.R. 6866 § 2(4)(A).
[67] H.R. 6866 § 3(a)(1)–(3).
[68] *Id*.
[69] *Id*.
[70] H.R. 6866 § 3(a)(4).
[71] H.R. 6866 §§ 3(b)–(e), 6.
[72] S. 3663, 116th Cong. § 3(a) (2020).
[73] S. 3663 § 3(d)–(h).
[74] S. 3663 § 4(b)(3), § 3(b).

does not apply to data collected by employers.[75]

According to Skopos Labs, Inc., which predicts the probability that a bill will pass both chambers of Congress, the PHEPA and the CCDPA each have only a two percent chance of enactment.[76] However, some experts say that there is a chance that one of the bills will pass.[77] Large technology companies, including Facebook, Microsoft, Apple, and Google, have expressed their support for comprehensive federal privacy law.[78]

B. THE EEOC AND THE AMERICANS WITH DISABILITIES ACT

Besides the FIPPs, federal agencies and laws must also be considered when thinking about information privacy law as it relates to health information. The EEOC and the ADA are relevant for the purposes of creating a contact tracing application that does not infringe on individuals' right to health privacy.

The EEOC is a federal agency responsible for enforcing laws prohibiting discrimination in hiring practices on the basis of "race, color, religion, sex, national origin, age, disability, and genetic information."[79] Laws enforced by the EEOC apply to hiring, firing, promotions, harassment, training, wages, and employee benefits.[80] Among the laws and regulations enforced by the EEOC, the ADA is one of the most important protections for employees.[81] The ADA requires employers to reasonably accommodate employees with statutory disabilities and to refrain from discriminating against prospective and current employees on

---

[75] S. 3663 § 2(12)(B), § 3(b).
[76] H.R. 6866, 116th Cong.; S. 3633, 116th Cong.
[77] Thomas Germain, *New Privacy Bills Aim to Protect Health Data During the Pandemic*, CONSUMER REPORTS (May 14, 2020), https://www.consumerreports.org/health-privacy/dueling-coronavirus-privacy-bills-could-protect-your-data-during-the-pandemic/.
[78] Mitchell Noordyke, *Big Tech's Shift to Privacy*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/big-techs-shift-to-privacy-2/ (last visited Dec. 5, 2020).
[79] *Overview*, EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/overview (last visited Sept. 20, 2020).
[80] *Id*.
[81] 42 U.S.C. §§ 12111-12117.

the basis of disability.[82] Although the ADA does not specifically name all of the impairments that constitute disabilities, it defines individuals with disabilities as having "a physical or mental impairment that substantially limits one or more major life activities," "a record of such impairment," or describes those who are "regarded as having such an impairment."[83] An individual may establish that they have a disability and are entitled to be covered pursuant to the ADA under one or more of these prongs.[84] Under the first prong, the standard "substantially limits" is meant to be construed broadly and is not a demanding standard.[85] Generally, this standard refers to activities that are substantially limited as compared to most people in the population. An impairment need not "prevent, or significantly or severely restrict" an individual from performing a major life activity, but rather less drastic interruptions to daily life can be considered substantially limiting.[86] Further, an impairment can be labelled a disability even when there are no symptoms. In *Bragdon v. Abbott*, the Supreme Court ruled that the Human Immunodeficiency Virus is a disability, even before the onset of the symptomatic phase of the virus, holding that certain major life activities, such as the ability to reproduce, may still be substantially limited.[87]

The EEOC has not stated whether it will consider COVID-19 to be a disability under the ADA; however, states with relatively more expansive disability protections, including New York, have labelled the virus a disability, and there has been at least one lawsuit requesting that it be considered as such.[88] In

---

[82] 42 U.S.C. § 12112(d)(4)(A).
[83] *See* 29 C.F.R. § 1630.2(g)(1); *see also* UNITED STATES DEP'T OF JUSTICE, CIVIL RIGHTS DIVISION, INFORMATION AND TECHNICAL ASSISTANCE ON THE AMERICANS WITH DISABILITIES ACT, https://www.ada.gov/ada_intro.htm (last visited Nov. 5, 2020).
[84] 29 C.F.R. § 1630.2(g)(2).
[85] 29 C.F.R. § 1630.2(j)(1)(i).
[86] 29 C.F.R. § 1630.2(j)(1)(ii).
[87] Bragdon v. Abbott, 524 U.S. 624, 638 (1998); 42 U.S.C § 12102(1); 29 C.F.R. § 1630.2(h)(2)(i).
[88] *Is COVID19 A Disability Under Discrimination Law? The Next Wave of Workplace Lawsuits May Answer Questions*, FISHER PHILLIPS (June 19, 2020) https://www.fisherphillips.com/resources-alerts-is-covid-19-a-

Tihara Worthy v. Wellington Estates, an employee alleged that she was wrongfully terminated and prevented from returning to work because of her previous COVID-19 positive status.[89] The plaintiff sought to have COVID-19 be considered a disability under New Jersey law.[90] The ADA restricts an employer's ability to ask potential or current employees about their disabilities and to require medical examinations.[91] It also prohibits employers from excluding individuals with disabilities unless they pose a significant risk of harm to other employees within the company,[92] and requires reasonable accommodations for individuals with disabilities during epidemics and contagious viral outbreaks, including permitting working from home.[93]

Although it is unclear whether COVID-19 will be considered a statutory disability, protections still exist for those who contract the virus.[94] For example, leave must be provided to employees who test positive for COVID-19.[95] The ADA also limits inquiries into the health of employees and the medical examinations that employers are able to conduct.[96] EEOC laws continued to apply during the COVID-19 pandemic, and it had continued to issue guidance regarding permissible treatment by employers during the COVID-19 pandemic. The EEOC has issued

---

disability-under-discrimination [hereinafter *Workplace Lawsuits*]; U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, TRANSCRIPT OF MARCH 27, 2020 OUTREACH WEBINAR (2020).

[89] *See* Workplace Lawsuits, *supra* note 88 (discussing Tihara Worthy v. Wellington Estates LLC). This case has been filed in the New Jersey Superior Court on June 15, 2020; *COVID-19 as a Covered Disability under New Jersey Law*, MASHEL LAW, LLC (Aug. 31, 2020), https://www.newjerseyemploymentattorneysblog.com/covid-19-as-a-covered-disability-under-new-jersey-law/.

[90] Workplace Lawsuits, *supra* note 88.

[91] *Id*.

[92] 42 U.S.C. §§ 12111(3), (8); 29 C.F.R. §§ 1630.2(r), 1630.15(b)(2).

[93] 42 U.S.C. § 12112(b)(5); *see also* § 12111(3); 29 C.F.R. § 1630.2(r); Strass v. Kaiser Found. Health Plan of Mid-Atlantic, 744 A. 2d 1000, 1007 (D.C. 2000) (noting that a reasonable accommodation can include job restructuring and reassignment to a vacant position).

[94] Id.

[95] Id.

[96] 42 U.S.C. § 12112(d)(4)(A).

guidance concerning potentially permissible medical examinations under the ADA in light of the pandemic, clarifying that temperature screenings and requirements to receive a negative COVID-19 test are allowed,[97] but tests for anti-bodies constitute impermissible medical examinations because they do not meet the ADA's standards.[98] The EEOC has noted that COVID-19 constitutes a "direct threat" under the ADA, allowing employers to make more "robust medical inquiries than would normally be allowed."[99] However, EEOC guidance is preempted by CDC guidance and state public health authorities.[100]

The ADA also offers guidance about storing employee medical information, including employee statements regarding the status of their COVID-19 infection or their suspicion of infection.[101] Additionally, employers may disclose the name and PII of employees suffering from COVID-19 to public health agencies, such as a state's Department of Health or the CDC.[102] However, employers may not specifically name the infected employee to other employees, but may generally inform others that there was a positive case within their vicinity.[103] This makes contact tracing applications popular tools for tracking the positive

---

[97] *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, EQUAL EMP. OPPORTUNITY COMM'N (Sept. 8, 2020) [hereinafter *What You Should Know About COVID-19*] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[98] *See id.*; *see also* Conroy v. New York State Department of Correctional Services, 333 F.3d 88, 93 (2d Cir. 2003) (noting that medical examinations cannot be required unless such examination is shown to be "job-related and consistent with business necessity").

[99] Taylor Eric White et al., *Employer Use of Contact Tracing Apps: The Good, the Bad, and the Regulatory*, LEXBLOG (July 7, 2020), https://www.lexblog.com/2020/07/07/employer-use-of-contact-tracing-apps-the-good-the-bad-and-the-regulatory/ (citing *Pandemic Preparedness in the Workplace and the Americans with Disabilities Act*, EQUAL EMP. OPPORTUNITY COMM'N (Mar. 21, 2020), https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act).

[100] *What You Should Know About COVID-19*, *supra* note 97.

[101] Joan Farrell, *Testing, Exams, and Medical Information*, ADA COMPLIANCE GUIDE ¶ 133 (2020), Westlaw 10992547.

[102] *Id.*

[103] *Id*.

spread of COVID-19 among employees within a company.[104]

The Occupational Safety and Health Administration ("OSHA") is a large regulatory agency under the United States Department of Labor, and has worked with the EEOC and the ADA to help maintain safe work environments during the COVID-19 pandemic.[105] Under OSHA's general duty clause, employers must provide a place of employment that is "free from recognized hazards that are causing or are likely to cause death or serious physical harm", and this includes protection from COVID-19 infection during work.[106] Although contact tracing is not explicitly mentioned in published guidelines for employers, OSHA recommends a combination of the use of personal protective equipment ("PPE"), administrative controls such as changes in work schedules to stagger employee arrival, and engineering controls such as installing products to minimize the spread of viruses, thereby implicitly allowing contact tracing to be utilized.[107]

The CDC has also published guidance regarding digital contact tracing, including that data should be "secure and confidential, be able to receive input from public health authorities, facilitate identification of known contacts, and be able to send notifications of exposure in multiple electronic formats."[108]

C. The Use of Contact Tracing Applications to Monitor the Spread of Respiratory Illness

Considering the guidance of the EEOC and health agencies, contact tracing can be instituted in the workplace. Employers may seek to keep their workplaces safe and abide by CDC guidelines by using contact tracing through the use of web and mobile

---

[104] *Id.*

[105] *See generally COVID-19*, OCCUPATIONAL SAFETY AND HEALTH ADMIN., https://www.osha.gov/SLTC/covid-19/ (last visited Oct. 11, 2020).

[106] 29 U.S.C. § 654 (1970); OCCUPATIONAL SAFETY AND HEALTH ADMIN., NO. 3990-03 2020, GUIDANCE ON PREPARING WORKPLACES FOR COVID-19, 4 (2020) [hereinafter OSHA Guidance] (noting that the General Duty clause applies to the COVID-19 pandemic).

[107] OSHA Guidance, *supra* note 106.

[108] White et al., *supra* note 99.

applications to identify, track, and warn the close contacts of infected employees.[109]

Contact tracing applications typically work by using Bluetooth or GPS technology to constantly broadcast strings of random numbers.[110] These numbers are broadcasted anonymously and change every few minutes.[111] When two electronic devices (such as cell phones) that have the application downloaded are in close contact for a specified amount of time, the two devices exchange their series of numbers and store these numbers within each phone's application.[112] When a user of an application tests positive for COVID-19, the application can let other users know that they were previously in close contact with someone who tested positive or exhibited symptoms of the virus.[113] Within the private sector, contact tracing applications may also link proximity or geolocation data with certain "personally identifiable information such as names and contact information."[114] In the employment context, applications can be used for both contact tracing within the company, and to ensure that employees abide by social distancing guidelines and other workplace rules.[115] When an employee contracts the virus, the application can inform other employees that they may have been exposed to the virus based on their physical location and proximity to the infected co-worker.[116]

These applications, which have already been used in several countries, by several U.S. states, and by various businesses

---

[109] Kelly Servick, *Cellphone Tracking Could Help Stem the Spread of Coronavirus. Is Privacy the Price*?, SCIENCE MAG (Mar. 22, 2020), https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price.

[110] *See, e.g.*, Stephen R. Brown et al., *May an Employer Require the Use of a Contact Tracing App?*, 38 NO. 01 WESTLAW J. COMPUT. & INTERNET 02 (2020).

[111] *Id*.

[112] *Id*.

[113] *Id*.

[114] JONES DAY, A GUIDE TO NAVIGATING CYBERSECURITY, PRIVACY, AND EMPLOYMENT LAW ISSUES WITH COVID-19 CONTACT TRACING IN THE PRIVATE SECTOR 1 (July 2020), https://www.jonesday.com/en/insights/2020/07/a-guide-to-navigating-cybersecurity-privacy-and-employment-law-issues-with-covid19-contact-tracing-in-the-private-sector.

[115] *Id*.

[116] *Id*.

in the United States,[117] may share proximity and geolocation tracking data to either a centralized or decentralized source.[118] Centralized methods use a computer server to match data and alert users, while the decentralized method stores data exclusively in each individual's phone.[119] Adopting the decentralized method renders a server powerless because Bluetooth tracking does not require personal information and leaves no trail back to users.[120] However, a centralized system involves the use and storage of personal data, and "puts the server in a position of trust, where it won't misuse" that personal information.[121] In other words, unlike a centralized model, a decentralized model would not tell an employee using the application where they were exposed.[122] Notably, the centralized model has been criticized on cybersecurity grounds as being easier to hack and manipulate.[123]

Although the ADA has not specifically commented on the

---

[117] *See* Patrick Howell O'Neill et al., *A flood of coronavirus apps are tracking us. Now it's time to keep track of them*, MIT TECH. REV. (May 7, 2020), https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/, for a database of countries using a COVID-19 contact tracing application; *see* Jefferson Graham, *Tracking coronavirus: Are Apple and Google contact tracing apps available in your state*?, USA TODAY, https://www.usatoday.com/story/tech/2020/10/02/apple-google-coronavirus-contact-tracing-apps/3592355001/ (Oct. 5, 2020, 2:06 AM), for the states that are using contact tracing applications; *see* Shannon Bond, *Your Boss May Soon Track You At Work for Coronavirus Safety*, NPR (May 8, 2020, 2:48 PM), https://www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety, for general information about contact tracing applications in the workplace.

[118] Daniel Kahn Gillmor, ACLU White Paper – *Principles for Technology-Assisted Contact-Tracing*, AMERICAN CIV. LIBERTIES UNION, (Apr. 16, 2020), https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing; Joseph Duball, *Centralized vs. decentralized: EU's contact tracing privacy conundrum*, INT'L ASS'N OF PRIV. PROS. (Apr. 28, 2020), https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/.

[119] Leo Kelion, *NHS rejects Apple-Google coronavirus app plan*, BBC News (Apr. 27, 2020), https://www.bbc.com/news/technology-52441428.

[120] Duball, *supra* note 118.

[121] *Id*.

[122] Gillmor, *supra* note 118.

[123] *Id*.

use of contact tracing, use of contract tracing applications would likely not be prohibited by the ADA provided that the application is not more intrusive than necessary to meet the business necessity standard.[124] To meet the business necessity standard, an employer that intends to require a medical examination must reasonably believe that an employee's behavior is a threat to vital functions of the business based on objective evidence.[125] A COVID-19 infection in the workplace would potentially create such a threat, as it can put employees at risk for contracting the virus. The way the applications will be implemented, however, will be almost entirely within each employer's control.[126] Under OSHA's General Duty Clause,[127] employers must provide a safe work environment, and COVID-19 has been labelled a disease that triggers employers' duties to take affirmative actions to reduce COVID-19 related hazards.[128] Along with guidance from OSHA and state and local health authorities, employers can implement additional precautions, such as contact tracing.[129]

II. DATA USE AND MISUSE

Outside of their immediate homes and communities, Americans come across the most social interaction, and thus their greatest potential exposure to COVID-19, at their workplace.[130]

---

[124] *GOING BACK TO WORK: EMPLOYER USE OF "APPS" ON EMPLOYEE PDAS/SMART PHONES FOR COVID-19 CONTACT TRACING*, ROPES & GRAY (MAY 1, 2020), https://www.ropesgray.com/en/newsroom/alerts/2020/05/Going-Back-to-Work-Employer-Use-of-Apps-on-Employee-PDAs-Smart-Phones-for-COVID-19-Contact-Tracing; *see* 42 U.S.C. § 12112(D)(4)(A).

[125] William Goren, *Job Relatedness and Business Necessity Revisited* (Jan. 5, 2018), https://www.understandingtheada.com/blog/2018/01/05/ada-job-related-business-necessity/ (citing Painter v. Illinois Department of Transportation, 715 Fed. Appx. 538, 541 (7th Cir. 2017)).

[126] *Id*.

[127] *See supra* note 106 and accompanying text.

[128] White et al., *supra* note 99.

[129] *Id*. (noting that OSHA requires that employers implement some combination of Personal Protective Equipment, cloth face coverings, administrative controls, and engineering controls).

[130] NATIONAL SAFETY COUNCIL, *POSITION/ POLICY STATEMENT - CONTACT TRACING*, https://nsc.org/getattachment/72ee1419-3d6b-41e2-a614-

Identifying infected employees, tracking their contacts at work, and sharing the information with public health agencies like the CDC can help to minimize exposure in the workplace and in the country as a whole, especially considering the fact that the United States lacks a national contact tracing mechanism.[131] There are no federal or state laws prohibiting employers from using contact tracing applications, and they can be readily initiated at workplaces around the United States.[132]

However, while digital contact tracing can be highly effective at controlling COVID-19 outbreaks,[133] provided that approximately 60 percent of the population installs a contact tracing application,[134] many Americans are worried about the implications of a contact tracing application at work.[135] Part II.A will examine privacy considerations and concerns as they relate to digital contact tracing applications. Part II.B discusses the potential for discrimination based on COVID-19 symptoms or infection through the use of digital contact tracing. Part II.C discusses the inadequate protection by the ADA in regard to the

---

3c31cadc9401/w-contact-tracing-161.

[131] *Id*.

[132] White et al., *supra* note 99.

[133] MATT J. KEELING, T. DEIRDRE HOLLINGSWORTH & JONATHAN M. READ, EFFICACY OF CONTACT TRACING FOR THE CONTAINMENT OF THE 2019 NOVEL CORONAVIRUS 861 (COVID-19) (2020).

[134] *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown*, UNIV. OF OXFORD. (Apr. 16, 2020), https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown ("We can stop the epidemic if approximately 60% of the whole population use the app and adhere to the app's recommendations. Lower numbers of app users will also have a positive effect; we estimate that one infection will be averted for every one to two users."); *see also* Sidney Fussell & Will Knight, *The Apple-Google Contact Tracing Plan Won't Stop Covid Alone*, WIRED (Apr. 14, 2020), https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone/ (noting that a successful contact tracing application needs fifty to seventy percent of the population to participate).

[135] *Digital Contact Tracing*, CORONAVIRUS TODAY, https://www.coronavirustoday.com/digital-contact-tracing (noting that in an online survey of 2000 people, 71 percent said they would not download a contact tracing application, and 44 percent of that group cited privacy concerns as the main reason).

COVID-19 pandemic and the personal health information of employees.

A. Information Privacy Considerations

Major privacy concerns related to digital contact tracing include whether employees will have sufficient notice and means to choose and consent to digital contact tracing within the workplace, the quality and standardization of the data collected through contact tracing applications, and how the information collected will be used and to whom it will be shared.

1. Choice/Consent and Notice/Awareness

Whether privacy policies for digital applications used by employers will adopt the common FIPPs is an important consideration for those who worry about the safety and security of their personal information, particularly in regard to the notice and awareness, and the choice and consent principles.[136] Without the meaningful application of the notice and awareness principle in a digital contact tracing application, employees may not get a sufficient amount of information about the collection and use of their personal information.[137]

Notice is also particularly important because, without it, individuals cannot constructively consent to privacy policies. In *Opperman v. Path Inc.*, the Northern District Court of California found that there were material issues of fact as to the scope of consent obtained by Yelp Inc. and whether there was sufficient consent for Yelp Inc.'s practice of uploading users' phone contacts.[138] The court noted that consent is only effective if the user agreed "to the particular conduct, or to substantially the same

---

[136] Aaron M. Baird, Kellen Mermin-Bunnell & Jacon Lesandrini, *Ethics of Digital Contact Tracing by U.S. Employers during the COVID-19 Pandemic*, HEALTH MGMT. POL'Y & INNOVATION (Apr. 30, 2020), https://hmpi.org/2020/04/30/ethics-of-digital-contact-tracing-by-u-s-employers-during-the-covid-19-pandemic-4-30-gsu-and-wellstar/.

[137] Camillo & Kornbacher, *supra* note 20, at 3.2-III.

[138] Opperman v. Path Inc., 205 F. Supp. 3d 1064, 1081 (N.D. Cal. 2016).

conduct," and that Yelp, Inc. did not explicitly mention that it would upload contact information.[139] Similarly, with the changing guidelines on sharing positive COVID-19 cases, employers would be unable to give adequate notice and could not solicit consent from employees.[140] Thus, employers may not have the ability to give notice of potential government and third party uses of the data collected from employees, and employees may not have the meaningful choice to resist the third party uses.[141] Without proper and conspicuous notice, employees cannot meaningfully consent to the use and disclosure of their PII, regardless of whether the application in question utilizes an opt-in or opt-out model of consent.[142] Moreover, it is likely that applications will require blanket consent at the outset due to the ongoing nature of employees' engagement with contact tracing applications.[143] This means that employees may be expected to consent broadly to future data disclosure and uses without fully understanding them. In other words, "because the consequences of granting blanket consent to use one's PII cannot be known at the time the consent is granted, this mechanism does not allow an individual to exercise meaningful control over disposition of his PII."[144]

There are a number of concerns relating to notice/awareness and choice/consent regardless of whether the use of a digital application is mandated or completely voluntary. In the absence of federal information privacy law on this matter, it is unknown whether employers can mandate the participation in

---

[139] *Id*. at 1077.
[140] Camillo & Kornbacher, *supra* note 20, at 3.2-III; U.S. Department of Labor Issues Enforcement Guidance For Recording Cases of COVID-19, OCCUPATIONAL SAFETY AND HEALTH ADMIN. NATIONAL NEWS RELEASE (U.S. Dep't of Labor, Washington, D.C.), April 10, 2020 [hereinafter OSHA NEWS RELEASE].
[141] Camillo & Kornbacher, *supra* note 20, at 3.2-III; OSHA NEWS RELEASE, *supra* note 140.
[142] John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 633 (2018).
[143] *Id.*; Brown et al., *supra* note 110.
[144] Rothchild, *supra* note 142.

digital contact tracing.[145] However, it is not expressly forbidden.[146] Mandatory use of contact tracing applications will effectively remove employees' ability to consent completely, because the privacy policies will be completely at the judgment of employers. Even if the application is facially voluntary, incentives and coercion may unduly influence employees to participate. Because of a perceived or actual lack of choice regarding the use of an application, employees may be stripped of the ability to meaningfully exercise choice and give consent, especially considering the tough economic climate, riddled with business closures and layoffs during the COVID-19 pandemic.[147] Conversely, some experts note that contact tracing technology will be significantly less effective if employees are able to opt-in or opt-out of using the technology and sharing their data.[148] This is because a significant number of employees must participate in digital contact tracing for it to be effective, and if too many employers opt-out, or fail to opt-in, digital contact tracing will not work as intended.[149]

The privacy notices given to employees are also at issue. If privacy notices are open-ended and broad, the resulting consent is less valid because it would be an agreement to a vague set of terms.[150] Alternatively, if an employer provides excessive detail in privacy notices regarding the anticipated uses, procedures, and goals for the data, constructive consent is also not guaranteed because employees may be overwhelmed by the information given,

---

[145] Brown et al., *supra* note 110.
[146] *Id.*
[147] *COVID-19's Serious Risks for Economic Rights*, Human Rights Watch (June 29, 2020), https://www.hrw.org/news/2020/06/29/covid-19s-serious-risks-economic-rights#.
[148] John Egan, *Contact-Tracing Apps Can Keep Tabs on Coronavirus*, SHRM (May 12, 2020), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/contact-tracing-apps-can-keep-tabs-on-coronavirus.aspx (referring to contact tracing applications as "safety devices.").
[149] Chiara Farronato, et al., *How to Get People to Actually Use Contact Tracing Apps*, HARVARD BUS. REV. (July 5, 2020), https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps.
[150] Determann, *supra* note 13.

especially with a lack of legal experience.[151] Moreover, according to a study by Deloitte, over ninety percent of people do not read privacy policies and other terms and conditions, citing complicated language and lack of meaningful choice in using the application or other digital platforms.[152] In another study, researchers created a fake social networking application and wrote corresponding terms and conditions in which users would have to agree to give up their first born child; 98 percent of users agreed to the terms.[153] The study suggested that privacy policies can take up to thirty minutes for users to read, and most people were not up to the task.[154] Moreover, employers may run into issues if they fail to explain privacy policies, or otherwise fail to provide adequate notice that they exist. In *Nguyen v. Barnes and Noble Inc.*, the Ninth Circuit reasoned that while failing to read policies is not a defense, entities that provide no notice, other than a conspicuous link to a set of policies, do not alone give users constructive notice of those policies.[155] Thus, simply having a privacy policy for a contact tracing application, even one that sufficiently addresses the uses the data will be put to, is not enough to solicit meaningful consent.

2. Proximity Information and Data Quality

Another criticism of digital contact tracing is that there is no consensus on how to standardize proximity data received from Bluetooth contact tracing mechanisms.[156] Standardization of data

---

[151] *Id.*; *see also* Brooke Auxier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/ (noting that only 9% of adults in the United States read privacy policies before agreeing to the terms).
[152] Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements* (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.
[153] JONATHAN A. OBAR & ANNE OELDORF-HIRSCH, THE BIGGEST LIE ON THE INTERNET: IGNORING THE PRIVACY POLICIES AND TERMS OF SERVICE POLICIES OF SOCIAL NETWORKING SERVICES 12 (2018).
[154] Id.
[155] Nguyen v. Barnes and Noble Inc., 763 F.3d. 1171, 1178-79 (9th Cir. 2014).
[156] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.

is the process of compiling different variables into one data set.[157] In this case, standardization is especially difficult when compiling confirmed positive cases of COVID-19, and symptoms reported by individuals without positive results, as well as compiling proximity data and data relating to the duration of exposure.[158] Additionally, it is especially difficult to compile accurate data to identify exposure to asymptomatic cases, because asymptomatic patients are less likely to confirm that they are positive for COVID-19.[159] This makes the accuracy and reliability of contact tracing data variable at best.[160] Additionally, whether contact tracing applications will rely on objective or subjective data is relevant in determining the accuracy of contact tracing mechanisms.[161] Using subjective data, such as the self-reporting of symptoms and suspected cases of COVID-19, dampens the accuracy of contact tracing because it is unclear whether those cases are positive or not.[162] However, using only objective data, such as authenticated test results puts the onus on people to get tested for COVID-19, whether or not they have symptoms.[163]

The quality of information received by contact tracing applications is further at issue for being overprotective.[164]

---

[157] Jim Frost, *Standardization*, https://statisticsbyjim.com/glossary/standardization/ (last visited Dec. 22, 2020).
[158] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.
[159] Caroline Chen, *America Doesn't Have a Coherent Strategy for Asymptomatic Testing. It Needs One***,** PROPUBLICA (Sept. 1, 2020), https://www.propublica.org/article/america-doesnt-have-a-coherent-strategy-for-asymptomatic-testing-it-needs-one (noting that asymptomatic patients were less likely to get tested and that there was no coherent strategy to test asymptomatic patients).
[160] Ashkan Soltani, Ryan Calo & Carl Bergstrom, *Contact tracing apps are not a solution to the COVID-19 crisis*, Brookings (Apr. 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.
[161] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.
[162] *Id.*; *What are common misconceptions about contact tracing?* (last updated Oct. 24, 2020), https://covid19.nj.gov/faqs/nj-information/slowing-the-spread/what-are-common-misconceptions-about-contact-tracing#direct-link (suggesting that New Jersey's exposure notification application will only use positive test results when notifying close contacts).
[163] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.
[164] *Cuomo Debuts New Contact Tracing, COVID Alert App as New York Battles*

Bluetooth signals can travel through walls, and as long as users are within six feet of each other, the contact tracing application will log the proximity data even though there is no risk of COVID-19 transmission.[165] On the other hand, when a user that does not receive alerts through the application when someone with COVID-19 was nearby, either because the application does not use push notifications or alerts or because there have been no reported cases within six feet of the user, a false sense of security may arise and users may feel less of a need to take precautions, such as using PPE or staying home from work when experiencing symptoms.[166] At work, employees may also choose or be required to leave their phones in another location, may turn their phones off during meetings or working hours, may experience bad Wi-Fi connection or signal during work, or may simply forget to charge their phone or bring their phone to work on any given day.[167] In these situations, a digital application would also be ineffective.

These accuracy problems cannot be solved by applications alone; most applications being developed create identification numbers for users that are not traceable, and there can be no way to verify accuracy.[168] Thus, there is a sizable risk of inaccurate proximity data.

3. Information Use and Sharing

Much of the worry regarding contact tracing applications is the potential for sharing data to third parties, including advertising companies or law enforcement agencies, as well as the theft or loss

---

Clusters, NBC N.Y. (Updated Oct. 2, 2020), https://www.nbcnewyork.com/news/coronavirus/cuomo-debuts-new-contact-tracing-covid-alert-app-as-new-york-battles-clusters/2646436/.

[165] *Id.*; Teresa Scassa, Jason Millar & Kelly Bronson, *Privacy, Ethics, and Contact Tracing Apps*, VULNERABLE: THE LAW AND POLICY OF COVID-19, 6 (Colleen M. Flood et al. eds., 2020) (citing Rob Kitchin, *Using Digital Technologies to Tackle the Spread of the Coronavirus: Panacea or Folly*, MAYNOOTH UNIV. (Apr. 21, 2020).

[166] Soltani, Calo & Bergstrom, *supra* note 160.

[167] White et al., *supra* note 99.

[168] *Id.*

of data.[169] However, many information privacy and data protection concerns related to digital contact tracing are not new. People have already become comfortable with opting into the location services of various applications, for example, and share personal data with applications and websites on a daily basis that can then be sold to advertisers or other third parties.[170] Digital contact tracing applications create the same risks for users; without sufficient controls, a log of a user's proximity to other users, as well as users' health status, can be used and disclosed to third parties.[171] Although individuals may be comfortable giving up information on other digital applications, they may not be willing to share their information when it involves their health.[172]

PII has long been protected by statutes such as the ADA and the Health Insurance Portability and Accountability Act ("HIPAA").[173] However, HIPAA typically does not apply in the employment context because it only concerns "covered entities," which include health care providers, health plans, and healthcare clearinghouses.[174] Most employers do not qualify as covered

---

[169] Adam Schwartz, *Two Federal COVID-19 Bills: A Good Start and a Misstep*, ELEC. FRONTIER FOUND. (May 28, 2020), https://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep; *see also* Todd Ehret, *Data Privacy Laws Collide With Contact Tracing Efforts; Privacy is Prevailing*, REUTERS (Jul. 21, 2020), https://www.reuters.com/article/bc-finreg-data-privacy-contact-tracing/data-privacy-laws-collide-with-contact-tracing-efforts-privacy-is-prevailing-idUSKCN24M1NL (noting that the Federal Bureau of Investigations has reported an increase in cyber-attacks during the COVID-19 pandemic).

[170] Andrew Crocker, Kurt Opsahl, & Bennett Cyphers, *The Challenge of Proximity Apps for COVID-19 Contact Tracing*, ELEC. FRONTIER FOUND., (Apr. 10, 2020), https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.

[171] *Id.*

[172] *Id.*

[173] White et al., *supra* note 99.

[174] *Id.*; *Covered Entities and Health Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Nov. 3, 2020). It also applies to "business associates," which are defined as any third parties that help a covered entity carry out its functions, including organizations that transmit PII to Covered Entities; White et al., *supra* note 99.

entities or business associates.[175] Besides the protection offered by the ADA, there is a competing legal obligation to report notifiable diseases to public health agencies such as the CDC and state-specific agencies.[176] Such reported information has traditionally been "kept private by public health agencies and then reported in the public domain either in aggregate or in other non-identifiable ways."[177] However, the use of a third-party application, and more specifically a contact tracing application, can disrupt the fine line between privacy and reporting requirements. A few questions arise, including who holds the right to access digital contact tracing information, whether the information could impact insurance rates or access to resources, for example, and whether work requirements will be affected for those who test positive for COVID-19.[178]

B. Potential for Discrimination and Lack of Accessibility

The potential for employment discrimination on the basis of COVID-19 infection, other related effects of the virus, or the refusal to use an application is important to consider in addition to information privacy and data protection concerns. With the use of contact tracing applications by employers, there may be risks of denied benefits and lack of workplace access for those who refuse to give consent to share their data or use a particular contact tracing application.[179] If the use of a contact tracing application is voluntary, employers can make it an opt-in or opt-out system in which employees will decide for themselves if they wish to participate.[180] Although this will give employees more decision-making ability and independence, without sufficient anti-discrimination mechanisms in place, this may prevent a sufficient number of people from opting-in or entice a large number of

[175] White et al., *supra* note 99.
[176] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.
[177] *Id.*; White et al., *supra* note 99.
[178] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.
[179] Schwartz, *supra* note 169.
[180] *See supra* notes 30-32 and accompanying text (describing opt-in and opt-out mechanisms).

employees to opt-out.[181] Employees may fear that their health status will exclude them at work, or deny them benefits consistent with working at the office.[182] For example, employees who test positive for COVID-19 may fear the stigma associated with it, and consequently fear that they will be excluded from attractive work opportunities[183], as employers may use health information to "refrain from hiring, retaining, or promoting job candidates."[184] If data is not sufficiently protected from theft or misuse, employers could be at risk for receiving higher rates for health, life, and disability insurance, banks could use it to make loan decisions, and landlords and housing associations could use the data to make tenant decisions.[185]

Other access-related concerns arise as well. Individual employees may not have cellphones with the capability of downloading and using a contact tracing application.[186] The application may also lack accessibility to people who are visually impaired, speak a different language, or are otherwise not familiar with legal jargon.[187] The August 2020 CCPA regulations provide that privacy notices must accommodate individuals with disabilities and those who speak languages other than English, but other proposed bills do not explicitly mandate this.[188]

C. Inadequate Protections by the ADA

---

[181] N.F. Mendoza, *Data researchers at odds: Will Americans opt in or opt out of COVID-19 contact tracing apps?*, TECHREPUBLIC (May 22, 2020), https://www.techrepublic.com/article/data-researchers-at-odds-will-americans-opt-in-or-out-of-covid-19-contact-tracing-apps/ (discussing a study in which 46 to 48 percent of Americans said they would opt out of using a contact tracing application).

[182] Baird, Mermin-Bunnell & Lesandrini, *supra* note 136.

[183] *Social Stigma Associated with COVID-19*, WORLD HEALTH ORG., https://www.who.int/docs/default-source/coronaviruse/covid19-stigma-guide.pdf.

[184] Determann, *supra* note 13.

[185] *Id.*

[186] Scassa, Millar & Bronson, *supra* note 165.

[187] *Id.*

[188] *See supra* notes 55-57 and accompanying text; *see* discussion *supra* Sections I.A.3, I.A.4 for information about state and federal information privacy bills.

Although EEOC guidance and the ADA govern, the EEOC has stated that its laws do not interfere with guidance issued by the CDC or local public health agencies regarding steps that employers should take to protect their workplace.[189] The changing guidance from health agencies and the unclear hierarchy between EEOC guidance and directions issued by public health authorities creates an unclear question for employers as to which guidance reigns supreme. Further, the EEOC's lack of direction about whether COVID-19 will be considered a disability under the ADA is leaving a gap open for abusive practices, considering that non-disabilities are not protected to the same extent.[190] In *Cossette v. Minnesota Power & Light*, the Eighth Circuit held that a plaintiff need not be disabled to state a claim for the unauthorized gathering or disclosure of confidential medical information under the ADA.[191] However, plaintiffs must also establish that a violation of the ADA caused tangible injury.[192] Because the misuse of confidential health information is not enough, employees may have a difficult time establishing tangible injury if they are discriminated against or their information is misused.

While they provide helpful guidance, EEOC publications do not address whether employers may mandate the use of digital contact tracing.[193] Employers are allowed to make disability-related inquiries and submit employees to medical examinations including mandatory COVID-19 testing and temperature scans before entering the workplace, because the pandemic was classified as a direct threat.[194] Additionally, the EEOC relied on CDC guidance and noted that employers may prevent employees from coming to work if they test positive or have symptoms of the virus.[195] Because of the allowance of certain medical examinations, and its endorsement by the CDC, it is likely that

---

[189] *What You Should Know About COVID-19*, *supra* note 97.
[190] U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, DISABILITY DISCRIMINATION [hereinafter EEOC Disability Discrimination] https://www.eeoc.gov/disability-discrimination (last visited Nov. 18, 2020).
[191] Cossette v. Minnesota Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999).
[192] *Id.*
[193] Brown et al., *supra* note 110.
[194] *Id.*; *see supra* note 99 and accompanying text.
[195] *Id.*

contact tracing is permissible under EEOC law, provided that it has not been expressly prohibited and does not constitute a medical examination that is more extensive than temperature checks or mandatory COVID-19 testing.

However, the most unclear aspect of the guidance released by the EEOC is that employers may follow the advice of local health agencies and the CDC regarding information needed to permit an employee's return to the workplace after travel.[196] Employers may also mandate doctor's notes for employees who say they cannot return to work.[197] In regard to the latter, the EEOC conceded that employees may need to rely on mechanisms other than healthcare professionals, who are generally busy during the pandemic, to generate an equivalent to a doctor's note.[198] It is unclear what an equivalent to a note from a medical professional is, and employers would have the power to decide what they will accept.

Employers must keep medical information confidential under the ADA, but the EEOC has stated that an employer may disclose the names of employees who test positive to OSHA.[199] However, assuming that a digital contact tracing application would broadcast and receive anonymous "pings" or proximity data, it would likely not be considered a disability inquiry under the ADA, because the numbers would not reveal employees' medical information.[200] Because this data is thus not protected by the ADA, it has the potential for abuse, especially if applications fail to sufficiently anonymize the data. The potential for abuse is twofold for applications that transmit data to the employer rather than keeping it on the user's phone in a decentralized manner.[201]

The EEOC's guidance implies that employers can ask employees to disclose whether employees received an exposure

---

[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION, REVISED ENFORCEMENT GUIDANCE FOR RECORDING CASES OF CORONAVIRUS DISEASE 2019 (COVID-19) (2020), https://www.osha.gov/memos/2020-05-19/revised-enforcement-guidance-recording-cases-coronavirus-disease-2019-covid-19.
[200] Brown et al., *supra* note 110.
[201] *See supra* notes 118-23.

alert notifying them that they were in close contact with COVID-19.[202] This has the potential for abuse, especially if employees ask about exposure alerts employees may have received when they were out of the office.[203] When employees receive an exposure alert, they may not know whether the exposure occurred in or out of the office because it will have been received after the exposure took place.[204]

Moreover, it is unclear if COVID-19 would be considered a disability under the ADA. Long-term effects of COVID-19 may include illnesses that would otherwise be considered statutory disabilities under the ADA,[205] as long as they substantially limit one or more major life activities, the individual suffering from such impairment has a record of it, or is regarded as having such impairment.[206] A major life activity can include the operation of a major bodily function.[207] The CDC has advised that long-term complications may severely affect cardiovascular, respiratory, renal, neurological, and cognitive functions to an extent yet unknown.[208] In some cases, patients suffered from permanent neurological damage and up to 40 percent of patients may suffer some neurological impairment, ranging from subtle changes in cognition to encephalitis, stroke, and dementia.[209] Moreover, many people who passed away from COVID-19 did not show neurological damage when they became infected, but later had brain damage when autopsies were performed.[210] Many of the potential conditions resulting from COVID-19 are permanent, and would otherwise be classified as disabilities.[211] However, the

---

[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] 42 U.S.C. § 12102(3)(A)
[206] 42 U.S.C. § 12102(1)
[207] 42 U.S.C. § 12102(2)(B)
[208] *Id.*
[209] Andrew M. Budson, *The Hidden Long-Term Cognitive Effects of COVID-19*, HARVARD HEALTH PUBL'G: HARVARD HEALTH BLOG (Oct. 8, 2020) https://www.health.harvard.edu/blog/the-hidden-long-term-cognitive-effects-of-covid-2020100821133 [hereinafter Long-Term Effects].
[210] *Id.*
[211] *Id.*

EEOC has failed to classify COVID-19 itself as a disability, leaving discrimination law under the ADA in limbo in regard to the pandemic.

Finally, the ADA does not presently prevent an employer from requiring employees to upload their list of "keys," or their sequence of randomly generated numbers which can show close-contact exposure.[212] Additionally, the CDC issued guidance stating that employers should inform the close contacts and other employees within the workplace if an employee tests positive.[213] While this should be anonymous, and the positive employee's name should not be given, the employee who tested positive will be missing from work during their quarantine, and thus their anonymity may be surrendered anyway.[214] This has potential for discriminatory practices, abuse, and associated stigma.

III. CONTACT TRACING AND PRIVACY OF HEALTH INFORMATION IN HARMONY

Although digital contact tracing implicates a number of privacy concerns, it is an invaluable tool for the control and eradication of viral outbreaks in the world at large. It is especially important that effective, yet secure, contact tracing can be used in the workplace to mitigate the effects of a pandemic on the economy and to ensure that businesses can stay open safely. Therefore, there must be a careful balancing to ensure that privacy concerns are mitigated, and digital contact tracing can be used in the workplace. Part III.A discusses why COVID-19 should be classified as a disability under the ADA, Part III.B endorses the PHEPA bill, Part III.C encourages states to pass broader privacy laws encompassing the FIPPs, and Part III.D discusses policies in the workplace which may make contact tracing safer and more effective.

A. Making COVID-19 a Disability under the ADA

---

[212] *Id.*
[213] *Id.*
[214] *Id.*

Much is still unknown about COVID-19 and its effects on the body.[215] The virus can present mild to no symptoms in some, and severe symptoms necessitating the need for hospitalization, intensive care, and the use of ventilators in others.[216] The risk of death or serious illness from COVID-19 increases with age, as well as for people with underlying conditions, such as diabetes, lung disease, obesity, and heart disease.[217] Although the ADA does not specifically list disabilities covered under it, long-term and chronic conditions are typically considered disabilities as long as the illness is a "physical or mental impairment that substantially limits one or more major life activities," the individual suffering from such impairment has a record of it, or is regarded as having such impairment.[218]

4. COVID-19 Fits the Statutory Definition of a Disability

The definition of "disability" is broadly construed in favor of covering individuals to the maximum extent permitted under the ADA.[219] Under this definition, many underlying conditions that may subject one to severe symptoms of COVID-19 are considered disabilities under the ADA.[220] A virus like COVID-19 making those conditions worse, or subjecting one to severe symptoms because of those disabilities, should also be considered a disability in these conditions.

However, COVID-19 can and should be labelled a disability on its own, without the existence of pre-existing conditions. Due to the potential and high-risk for serious long-term conditions, many of which can be categorized as disabilities on their own under the ADA, COVID-19 infection should itself be considered a disability. It would be proper to do so, as COVID-19

---

[215] *See generally* Kathy Katella, *5 Things Everyone Should Know About the Coronavirus Outbreak*, YALE MEDICINE (Nov. 17, 2020), https://www.yalemedicine.org/stories/2019-novel-coronavirus (explaining what is known about the virus); *see supra* notes 208-211 and accompanying text.
[216] *See supra* notes 209-211 and accompanying text.
[217] *See supra* notes 209–211 and accompanying text.
[218] *See supra* note 83 and accompanying text.
[219] 42 U.S.C. § 12102(4)(A).
[220] 42 U.S.C. § 12102(3)(A); *see supra* note 205 and accompanying text.

easily fits the first prong of the disability definition prescribed by the ADA. COVID-19 is a physical and mental impairment that causes difficulty breathing, impaired cognition, or "brain fog," fatigue, muscle and joint pain, and a range of long-term conditions.[221] These include neurological, musculoskeletal, respiratory, cardiovascular, immune, and circulatory conditions and suffice as physical and mental impairments.[222] All of these listed impairments are symptoms and effects of COVID-19 in a large number of people. Moreover, one need not have these symptoms to be considered physically or mentally impaired; it is enough that an employer may believe an employee has one or more of these impairments stemming from prior COVID-19 infection.[223]

COVID-19 also substantially limits one or more major life activities, because its symptoms and effects on the body may prevent people from going to work, from getting out of bed, and from living with the full use of their organs due to the burden of the virus on such organs.[224] Even if an employee is not actively exhibiting symptoms of these impairments, they may still reach the threshold for substantial limitation of a major life activity.[225] Because COVID-19 substantially limits the use of bodily functions,[226] and substantially limits major life activities, it meets the first prong of the definition of "disability" under the ADA.[227]

---

[221] Long-Term Effects, *supra* note 209; *see supra* notes 208–211 (discussing long-term conditions of the virus).
[222] *See supra* notes 208–211.
[223] *See supra* note 83 and accompanying text (noting that it is enough that an employer regards an employee as having a disability).
[224] *See supra* note 207 and accompanying text (noting that the disruption of a major bodily function can be a major life activity).
[225] Bragdon v. Abbott, 524 U.S. 624, 638 (1998); *see supra* note 87 and accompanying text.
[226] 29 C.F.R. § 1630.2(j)(1)(iv).
[227] Note that the word "major" is not interpreted strictly to create a demanding standard for disability, and is not determined by reference to whether the activity is of "central importance to daily life." 29 C.F.R. § 1630.2(i)(2).

5. Making COVID-19 a Statutory Disability would Protect Employees from Discrimination

Under the ADA, qualified individuals with disabilities are protected from unfavorable treatment by their employers.[228] Individuals with a history of a disability, or those believed by their employers to have a physical or mental impairment lasting six months or more, even if they do not have such impairment, are also protected.[229] The ADA protects such individuals from unfavorable treatment including selective hiring, firing, pay disparity, job assignment, promotions, layoffs, training, benefits, and other conditions of employment, as well as harassment for such disability or impairment.[230] If COVID-19 was labelled a disability under the ADA, individuals who contract it would be protected from unfair employment practices. This is especially important considering that digital contact tracing applications may notify employers when someone contracts the virus as it will have to be recorded and reported to public health agencies and to OSHA.[231] Further, individuals with disabilities are due reasonable accommodations, such as the ability to work from home for individuals with COVID-19 infections.[232]

B. Passing the PHEPA with FIPPs

The CCDPA and PHEPA apply to covered entities, which are entities that engage in contact tracing or exposure notification mechanisms.[233] Each bill requires covered entities to take steps to ensure privacy before and after collecting covered data and creates

---

[228] EEOC Disability Discrimination, *supra* note 190.
[229] *Id.*
[230] *Id.*
[231] *See supra* note 199 and accompanying text; OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION, OSHA INJURY AND ILLNESS RECORDKEEPING AND REPORTING REQUIREMENTS, https://www.osha.gov/recordkeeping/ (last visited Nov. 28, 2020).
[232] EEOC DISABILITY DISCRIMINATION, *supra* note 190.
[233] JONATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10501, "TRACING PAPERS": A COMPARISON OF COVID-19 DATA PRIVACY BILLS (2020); *see* discussion *supra* section I.A.4.

enforcement mechanisms to ensure that entities comply with their obligations.[234] However, major differences arise between the CCDPA and the PHEPA bills in regard to the data that is covered.

6. The PHEPA Should be Passed Instead of the CCDPA

The CCDPA insufficiently covers data collected by contact tracing applications, as it applies to the most narrow set of data, including only precise geolocation data, proximity data, persistent identifiers—or information that can identify individual users—and personal health information.[235] The CCDPA also excludes data collected by covered entities concerning anyone "permitted to enter a physical site of operation of the entity," including employees.[236] The PHEPA, on the other hand, would protect any information actually linked or reasonably linkable to individuals or devices that is collected, processed, or transferred as part of a digital contact tracing mechanism, and applies to all exposure notification mechanisms, not just those related to the COVID-19 pandemic.[237] The PHEPA similarly protects a greater range of data, and creates a private right of action for violations, which the CCDPA fails to do.[238] The PHEPA provides more protection for the privacy of employee's medical data and information received from digital contact tracing applications.[239]

7. Enforcing the FIPPs

The PHEPA also more broadly encompasses the FIPPs, which offer higher protection for information collected through

---

[234] *See* discussion *supra* section I.A.4.
[235] *See* discussion *supra* section I.A.4.
[236] *See* discussion *supra* section I.A.4.; S. 3663, 116th Cong. § 10 (2020).
[237] GAFFNEY, *supra* note 233.
[238] *Id.*
[239] Suzan DelBene, *Combatting COVID While Protecting Privacy: the Public Health Emergency Privacy Act (PHEPA)*, https://delbene.house.gov/uploadedfiles/public_health_emergency_privacy_act_-_one_pager.pdf (last visited Nov. 18, 2020); *Proposed Federal Privacy Legislation Tackles COVID-19 Data*, JD SUPRA (May 22, 2020), https://www.jdsupra.com/legalnews/proposed-federal-privacy-legislation-10027.

digital contact tracing applications. The PHEPA operates on an opt-in consent model, in which users of contact tracing applications would have to affirmatively consent to the use of their data, and have the ability to revoke consent at any time, after which the employer would have to destroy the data and prevent it from being used or shared.[240] PHEPA also satisfies the access/participation principle, as it provides that there must be a reasonable attempt at ensuring the accuracy of data, and individuals must have the ability to correct their data.[241] The bill also stipulates that there must be reasonable safeguards to protect the confidentiality and security of data,[242] that data must be destroyed after the COVID-19 emergency is terminated, and that data should not be linked to individuals in a way that would identify them,[243] thus satisfying the integrity/security principle. The notice/awareness principle is met in § 3(e), requiring that organizations collecting, using, or disclosing health data should provide a clear and conspicuous privacy policy that describes how and for what purpose the data is collected, to whom it is disclosed, and the purpose of its disclosure.[244] It also specifies that the privacy policy must describe the organization's data retention and security policy, and explain how individuals can file complaints and exercise their rights under the proposed act.[245] Finally, the enforcement/redress prong is met in § 6, where it describes how states, the FTC, and private citizens can seek redress for data breach.[246] Outside of the FIPPs, PHEPA also allows for data minimization and anti-discriminatory practices.[247]

The CCDPA, on the other hand, does not meet the minimum standards under the FIPPs, and fails to cover a wide range of data, including data collected by employers.[248] Its state

---

[240] Schwartz, *supra* note 169; H.R. 6866 §§ 3(d), 3(d)(2)(A).
[241] H.R. 6866 § 3(a)(2); *see* discussion *supra* section I.A.4.
[242] H.R. 6866 § 3(b); *see* discussion *supra* section I.A.4.
[243] H.R. 6866 §§ 3(g)(1)(A), 3(g)(2); *see* discussion *supra* section I.A.4.
[244] H.R. 6866 § 3(e); *see* discussion *supra* section I.A.4.
[245] H.R. 6866 § 3(e)(3), (4); *see* discussion *supra* section I.A.4.
[246] H.R. 6866 § 6; *see* discussion *supra* section I.A.4.
[247] H.R. 6866 §§ 3(a)(1), 3(a)(3); *see* discussion *supra* section I.A.4.
[248] Schwartz, *supra* note 169; S. 3663, 116th Cong. § 6(B)(iv) (2020); *see* discussion *supra* section I.A.4.

law preemption provision would "cut back" the legal rights of individuals in states with broad data privacy laws, including Californians under the CCPA.[249] This would cut back rights to access data under the access/participation principle and prevent the right to delete or opt-out of data under the choice/consent principle.[250] The CCDPA also lacks a private right of action, under the enforcement/redress principle, which would severely limit how individuals could get redress from data breach.[251]

C. Passing State Information Privacy Laws Related to Contact Tracing

If Congress takes no action, information collected by digital contact tracing applications may be subject to state privacy regulations, which only exist in some states and often fail to offer full privacy protection.[252] The CCPA is currently the most protective and broad statute governing the privacy of consumers, and other states should follow suit. State law should model California's CCPA, or should be amended to expressly provide for a mandatory explanation of privacy policies and avenues for redress, the permitted use of subjective and objective data in contact tracing applications with accurate labels, the disallowance of GPS tracking, and a decentralized model for data storage.

8. Adequate Application of the Notice/Awareness Principle

Beyond a clear and conspicuous written privacy policy, a verbal explanation of privacy policies involving digital contact tracing applications should be available for employees to fully enjoy the notice/awareness principle under the FIPPs. To ensure that users of digital contact tracing applications actually understand and know about the application's privacy policies and avenues of redress in case of data breach or misuse, the policies should be

---

[249] *See* discussion *supra* section I.A.4.
[250] Schwartz, *supra* note 169; S. 3663, 116th Cong. § 3 (2020).
[251] Schwartz, *supra* note 169; see *supra* notes 72-75 and accompanying text for a discussion of the CCDPA.
[252] *See* discussion *supra* section I.A.3.

conspicuous, clear, without legal jargon, and available to people with disabilities and those who speak different languages, just like the CCPA provides.[253] Otherwise, the notice/awareness principle is implicitly violated, and users consequently cannot exercise their right to opt-in or opt-out.

9. Proximity Data Tracking and Storage

The use of subjective data in digital contact tracing applications is another cause for concern.[254] Subjective data, such as the self-reporting of symptoms, can increase applications' inaccuracy, because it will be unknown whether those cases are positive or not.[255] However, preventing users from submitting subjective data can impede contact tracing efforts when, in the event of COVID-19 test shortages or long lines at testing centers, employees are unable to get tested before displaying symptoms. A potential solution is to allow both subjective and objective data, including mere symptoms and official COVID-19 test results, but labelling them as such in the application. This way, employees will still be informed of potential and actual risk of COVID-19, while seeing the potential severity of the exposure.

Further, using Bluetooth rather than GPS tracking would preserve users' information and prevent data breach and misuse. Although Bluetooth can be less accurate, as the signal can travel through walls and send employees false exposure notifications,[256] users' locations are not logged as part of the mechanism, making it less likely that users will be tracked and their health information released or misused.[257] With Bluetooth contact tracing, a user's temporary identification number rotates frequently, preventing third parties from tracking individual users over time.[258]

---

[253] *See supra* notes 152–154 (noting that people typically do not read privacy policies); *see supra* note 188 (discussing the 2020 CCPA regulations).
[254] *See supra* notes 161–163 and accompanying text.
[255] *See supra* notes 161–163 and accompanying text.
[256] *See supra* note 164 and accompanying text.
[257] JASON BAY ET AL., BLUETRACE: A PRIVACY-PRESERVING PROTOCOL FOR COMMUNITY-DRIVEN CONTACT TRACING ACROSS BORDERS (2020).
[258] *Id.*

Alternatively, GPS accuracy decreases indoors, where risk of transmission is much higher, and entire buildings may fall within the reporting range of a single GPS point.[259] Moreover, GPS tracking increases battery drain, which can curtail the accuracy of contact tracing in general.[260] Further, there are other privacy concerns associated with GPS tracking.[261] GPS tracking data consists of sensitive information about users' activities and locations, most of which is unrelated to public health purposes. Any repository of such data can present an encroachment on individual privacy.[262] Users can be identified with location tracking data, especially in sparsely populated areas where truly anonymizing data is futile.[263]

A decentralized model for contact tracing, in which the data stays on the user's phone rather than being transmitted to another database, is ideal to preserve privacy and prevent misuse by malignant actors.[264] Centralized systems operate with personal data, while the decentralized model will simply inform employees that they were exposed without offering information regarding where they were exposed, and from whom.[265]

10. Collaboration with the EEOC and Public Health Agencies

Finally, there should be continuous collaboration between states, the EEOC, and public health agencies so that employers can receive up-to-date information and can amend their privacy policies accordingly. In light of changing circumstances regarding

---

[259] *Id.*; Julian Sanchez & Matthew Feeney, *Protect Privacy When Contact Tracing*, CATO INSTITUTE: PANDEMICS AND POLICY (Sept. 15, 2020), https://www.cato.org/publications/pandemics-policy/protect-privacy-when-contact-tracing#best-technologies-determining-location-proximity.
[260] BAY ET AL., *supra* note 257.
[261] Sanchez & Feeney, *supra* note 259.
[262] *Id.*
[263] Jessica Davis, *COVID-19 Contact Tracing Apps Spotlight Privacy, Security Rights*, HEALTH IT SECURITY (May 20, 2020), https://healthitsecurity.com/news/covid-19-contact-tracing-apps-spotlight-privacy-security-rights.
[264] *See supra* notes 118–123 and accompanying text.
[265] *See supra* notes 118–123 and accompanying text.

COVID-19, states should receive updated information to issue guidance for employers about the pandemic and where and how information about infected employees should be shared. This will ensure that the notice/awareness principle is satisfied; employees can have updated privacy policies that match the guidance of the EEOC, the CDC, and local health agencies.

With these explicit additions to state and federal laws, digital contact tracing can offer far more protection to users and employees using digital contact tracing applications by informing users of exposure to COVID-19, while protecting their privacy and personal information.

D. In the Workplace

Many employers may have had mixed feelings about smartphones in the workplace, considering they may be distracting for employees. However, in light of the COVID-19 pandemic and contact tracing efforts, employers should encourage employees to carry their phones with them wherever they go. Additionally, to satisfy the notice/awareness and choice/consent principles, employers should verbally explain privacy policies as they are updated and amended. This would further ease employees into understanding and constructively opting-in or opting-out of contact tracing applications.

Further, employers should collaborate with the CDC and other health departments to implement a preparedness and response plan to consider actions in the event of an outbreak, collect information in the workplace consistent with privacy considerations, and conduct workplace hazard evaluation and prevention activities to prevent the spread of COVID-19 in the workplace.[266] Employers should also transparently communicate with their employees regarding privacy and anti-discrimination policies to allow employees to feel comfortable using digital contact tracing applications during work.

---

[266] CENTERS FOR DISEASE CONTROL, CASE INVESTIGATION AND CONTACT TRACING IN NON-HEALTHCARE WORKPLACES: INFORMATION FOR EMPLOYERS (2020).

CONCLUSION

COVID-19 and the necessity of digital contact tracing applications has brought many privacy issues to light. However, these concerns do not end with the eradication or mitigation of COVID-19. There will likely be other pandemics and disease outbreaks in coming years due to human behaviors like deforestation and encroachment on diverse wildlife habitats.[267] With these behaviors, humans will come in contact with other species and facilitate the spread of coronavirus illnesses.[268] Because of these factors, it is imperative that the world as a whole establishes mechanisms for effective contact tracing without an irresponsible imposition on the privacy of individuals using the mechanisms. To be proactive, privacy concerns with contact tracing must be mitigated now, before the next outbreak occurs.

[267] Victoria Gill, *Coronavirus: This is Not the Last Pandemic*, BBC (June 6, 2020), https://www.bbc.com/news/science-environment-52775386.
[268] *Id.*